



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,483	01/27/2004	Gun-il Lee	1793.1183	6277
21171 7590 09/16/2008 STAAS & HALSEY LLP SUITE 700 1201 NEW YORK AVENUE, N.W. WASHINGTON, DC 20005			EXAMINER NGUYEN, ALLEN H	
			ART UNIT 2625	PAPER NUMBER
			MAIL DATE 09/16/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/764,483

**Applicant(s)**

LEE, GUN-IL

**Examiner**

ALLEN H. NGUYEN

**Art Unit**

2625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 May 2008.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 6-11 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 6-11 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 27 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☒ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-8508)  
Paper No(s)/Mail Date \_\_\_\_\_  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_  
5) ☐ Notice of Informal Patent Application  
6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

- This office action is responsive to the following communication:  
Amendment filed on 05/21/2008.
- Claims 6-11 are currently pending in the application.

***Priority***

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

***Response to Arguments***

2. Applicant's arguments filed 05/21/2008 have been fully considered but they are not persuasive.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 6-11 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claim 6, the claim requires “storing the security information on the security server”, and “transmitting the security information and the document data to the receiving facsimile machine from the transmitted facsimile machine.” The specification does not support the security information is stored in the security server and a transmitting facsimile machine transmitted the security information in the security server to a receiving facsimile machine.

Regarding claims 7-11, claims 7-11 are rejected under 35 U.S.C. 112, first paragraph, as being depend on rejected base claims.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 6-11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 6, the claim requires “storing the security information on the security server”, and “transmitting the security information and the document data to the receiving facsimile machine from the transmitted facsimile machine.” The examiner does not know how the security information is obtained from the security server by the transmitting facsimile machine.

It is also unclear the security information of line 11 is referring to the security information stored in the security server or the security information transmitted by the transmitting facsimile machine.

Regarding claims 7-11, claims 7-11 are rejected under 35 U.S.C. 112, second paragraph, as being depend on rejected base claims.

Since the claim does not make sense to the examiner because of the 112 issue, the examiner is rejecting the claim base on one of the possible interpretation that make sense to the examiner.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 6-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry (US 6,385,728) in view of Stodder et al. (US 5,727,890).

Regarding claim 6, DeBry '728 discloses a method of selectively printing document data (File Source 10, fig. 3) using a security server (Certificate Authority 60, fig. 4), which provides security information on users (i.e., a certificate authority 60 to authenticate the user's digital certificate; Col. 9, lines 19-20) who are authorized to print document data transmitted from a transmitting facsimile machine (i.e., a fax machine

may be understood to be a printer; Col. 12, line19-20, fig. 3, Print Server 30) to a receiving facsimile machine (User/Client 20, fig. 3), to the receiving facsimile machine (User/Client 20, fig. 3), the method comprising:

storing the security information (i.e., the authority 60 includes a public key in the certificate given to the printer and encodes the corresponding private key with the secret key from the database; Col. 9, lines 63-65) on the security server (60, fig. 4);

transmitting the security information and the document data to the receiving facsimile machine (i.e., the printer may then send, 402, the public key and user identification to a certificate authority 60 to authenticate the user's digital certificate. The print system now has the user's public key and knows that it is authenticated. The printer sends, 403, to the user a random message; See col. 9, lines 18-23, fig. 4) from the transmitting machine (30, fig. 4);

receiving user information on a user attempting to print the document data (i.e., the user encrypts the message with its private key and sends, 404, it back to the printer; Col. 9, lines 23-24) at the receiving machine (User 20, fig. 4);

authenticating the user based on a result of comparing the received user information with the security information (i.e., the print system decrypts the message with the user's public key. If it matches the original message, then the printing system knows that the user is who the user purports to be; Col. 9, lines 24-27);

printing the document data if the user is authenticated at the receiving facsimile machine (i.e., the printer has verified the authentication and authority of the user 20, the

printer sends a file request to the server along with the will-call certificate, which is now encrypted with the printer's private key; Col. 9, lines 35-40),

wherein the security information is transmitted via a security communication line different from a communication line that transmits the document data from the transmitting facsimile machine to the receiving facsimile machine (i.e., it should be noted that the secret key built into the printer and stored in the database of the authority is only used between the printer and the authority for generating digital certificates. In such an embodiment, the secret key is not used for any other communications using traditional symmetric cryptography; Col. 10, lines 1-5).

It should be noted that Debry '728 does not explicitly show printing document data for facsimile machines.

However, the above-mentioned claimed limitations are well known in the art as evidenced by Stodder '890. In particular, Stodder '890 teaches printing document data for facsimile machines (i.e., a multiple-function printer/fax machine which is primarily a printer peripheral for a computer as well as primarily a fax machine, having an integrated, shared paper path and common mechanisms including a common chassis for scanning documents on the one hand and for producing hardcopy printout sheets on the other hand; Col. 2, lines 20-30).

In view of the above, having the system of Debry and then given the well-established teaching of Stodder, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the system of Debry as taught by Stodder to include: printing document data for facsimile machines, since Stodder

stated in col. 1, lines 40-50 that such a modification would ensure a fax machine acts primarily as both a sender (i.e., scanning and transmitting) and receiver of documents, and that the fax machine also acts secondarily as a printer (i.e., printing a facsimile of a second document, printing a copy of a scanned first document, or printing an itemized report) and secondarily as a convenience copier (i.e., scanning/printing a first document).

Regarding claim 7, DeBry '728 discloses the method, wherein the security information includes at least a plurality of identifications and passwords of the authorized users (i.e., access to resources of a computer system ("server") from another system or user ("user") has been controlled through passwords. This requires the server to maintain a database of all authorized users and each user's password; Col. 4, lines 15-20).

Regarding claim 8, DeBry '728 discloses the method, wherein the authenticating the user (User 20, fig. 4) based on a result of comparing the received user information (Digital Certificate, fig. 4) with the security information (Authenticates Certificate 402, fig. 4) comprises:

providing the received user information to the security server (i.e., in a certificate-based access control system, the server only needs to authenticate certificates issued by a certification authority; Col. 4, lines 22-24);



enabling the security server for the facsimile machines to determine whether to authenticate the unauthorized user based on a result of comparing the received user information with the security information and to inform the receiving facsimile machine of a result of the determination (i.e., to gain access to resources of the server, the user submits the user's certificate. From the certificate, which contains data that cannot be forged, the server can obtain the user's authenticated public number, personal data, and access privileges. The server can then transmit to the user a random message that the user must digitally sign with the user's private number and return it to the server. The server can then authenticate the digital signature using the public number in the certificate and check that the signed message is the same it sent to the user. With this digitally-signed response, the server can determine if the user has the correct private number corresponding to the authenticated public number in the certificate; See col. 4, lines 25-40).

It should be noted that Debry '728 does not explicitly show for using the facsimile machines.

However, the above-mentioned claimed limitation is well known in the art as evidenced by Stodder '890. In particular, Stodder '890 teaches for using the facsimile machines (i.e., a multiple-function printer/fax machine which is primarily a printer peripheral for a computer as well as primarily a fax machine, having an integrated, shared paper path and common mechanisms including a common chassis for scanning documents on the one hand and for producing hardcopy printout sheets on the other hand; Col. 2, lines 20-30).

In view of the above, having the system of Debry and then given the well-established teaching of Stodder, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the system of Debry as taught by Stodder to include: using the facsimile machines, since Stodder stated in col. 1, lines 40-50 that such a modification would ensure a fax machine acts primarily as both a sender (i.e., scanning and transmitting) and receiver of documents, and that the fax machine also acts secondarily as a printer (i.e., printing a facsimile of a second document, printing a copy of a scanned first document, or printing an itemized report) and secondarily as a convenience copier (i.e., scanning/printing a first document).

Regarding claim 9, DeBry '728 discloses the method, wherein the authenticating the user (User 20, fig. 4) based on a result of comparing the received user information (Digital Certificate, fig. 4) with the security information (Authenticates Certificate 402, fig. 4) comprises:

providing the received user information to the transmitting facsimile machine (i.e., the Print System 30 can obtain the user's authenticated public number, personal data, and access privileges; Col. 4, lines 28-30);

enabling the transmitting facsimile machine (i.e., a fax machine may be understood to be a printer; Col. 12, lines 20-21, fig. 4, Print System 30) to determine whether to authenticate the unauthorized user or not based on a result of comparing the received user information with the security information and to inform the receiving machine (User/Client 20, fig. 4) of a result of the determination (i.e., a user 20/Receiving

Machine will request the document from the Print System 30, the Print System will verify that the user has the correct access privileges, and if so, then the Print System will send a copy of the document to the user; col. 4, lines 50-55).

It should be noted that Debry '728 does not explicitly show the receiving machine is fax machine.

However, the above-mentioned claimed limitation is well known in the art as evidenced by Stodder '890. In particular, Stodder '890 teaches the receiving machine is fax machine (i.e., a multiple-function printer/fax machine which is primarily a printer peripheral for a computer as well as primarily a fax machine; Col. 2, lines 21-23).

In view of the above, having the system of Debry and then given the well-established teaching of Stodder, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the system of Debry as taught by Stodder to include: the receiving machine is fax machine, since Stodder stated in col. 1, lines 40-50 that such a modification would ensure Facsimile devices (i.e., fax machines) have been used for many years, to transmit documents containing text or graphical images through a modem via telephone lines through another modem to a remote destination.

Regarding claim 10, DeBry '728 discloses the method, wherein the authenticating the user (User 20, fig. 4) based on a result of comparing the received user information (Digital Certificate, fig. 4) with the security information (Authenticates Certificate 402, fig. 4) comprises:

providing the received user information to the receiving machine (i.e., the Print System 30 can transmit to the user a random message that the user must digitally sign with the user's private number and return it to the Print server; Col. 4, lines 30-32, fig. 4);

enabling the receiving facsimile machine to determine whether to authenticate the unauthorized user or not based on a result of comparing the received user information with the security information and to inform the receiving machine of a result of the determination (i.e., the server can then authenticate the digital signature using the public number in the certificate and check that the signed message is the same it sent to the user. With this digitally-signed response, the server can determine if the user has the correct private number corresponding to the authenticated public number in the certificate).

It should be noted that Debry '728 does not explicitly show the receiving machine is fax machine.

However, the above-mentioned claimed limitation is well known in the art as evidenced by Stodder '890. In particular, Stodder '890 teaches the receiving machine is fax machine (i.e., a multiple-function printer/fax machine which is primarily a printer peripheral for a computer as well as primarily a fax machine; Col. 2, lines 21-23).

In view of the above, having the system of Debry and then given the well-established teaching of Stodder, it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the system of Debry as taught by Stodder to include: the receiving machine is fax machine, since Stodder stated in col.

1, lines 40-50 that such a modification would ensure Facsimile devices (i.e., fax machines) have been used for many years, to transmit documents containing text or graphical images through a modem via telephone lines through another modem to a remote destination.

Regarding claim 11, DeBry '728 discloses a computer-readable medium encoded with processing instructions implementing the method (i.e., having computer-readable program code, may be embodied within one or more computer-usable media such as memory devices or transmitting devices, thereby making a computer program product; Col. 11, lines 20-25) of selectively printing document data (File Source 10, fig. 3) using a security server (Certificate Authority 60, fig. 4), which provides security information on users who are authorized to print document data transmitted from a transmitting facsimile machine (i.e., a fax machine may be understood to be a printer; Col. 12, line 19-20, fig. 3, Print Server 30) to a receiving facsimile machine (User/Client 20, fig. 3), to the receiving facsimile machine (User/Client 20, fig. 3).

### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Burkitt (US 6,195,348) discloses dynamic realtime protocol for facsimile and the like.

Sato et al. (US 6,704,775) discloses facsimile image information managing system and method.

Andivahis et al. (US 2003/0147536) discloses secure electronic messaging system requiring key retrieval for deriving decryption keys.

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALLEN H. NGUYEN whose telephone number is (571)270-1229. The examiner can normally be reached on M-F from 9:00 AM-6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, King Poon can be reached on (571)-272-7440. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/King Y. Poon/  
Supervisory Patent Examiner, Art Unit 2625

/Allen H Nguyen/  
Examiner, Art Unit 2625